

DEPARTMENT OF STATE
FISCAL YEAR 2008
PRIVACY IMPACT ASSESSMENT

Electronic Medical Record (EMR)

Conducted by:
Bureau of Administration
Information Sharing and Services
Office of Information Programs and Services
Privacy Office
E-mail: pia@state.gov

The Department of the State FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

The purpose of the new *requirements is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Section 208 of the E-Government Act requires that agencies now conduct Privacy Impact

Assessments (PIA) on all IT projects being planned, developed, implemented, and/or operating regarding individual.

Department of State Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

IT Project Name/Number: Electronic Medical Record (EMR)

Program Manager: Jim Thornberry

Telephone Number: 202-663-1758

E-mail Address: thornberryJM@state.gov

A. CONTACT INFORMATION:

Who is the Agency Privacy Coordinator who is conducting this assessment?
(Name, organization, and contact information).

**Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)**

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) **Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail addresses: pia@state.gov. If answer is yes, please complete the survey in its entirety.**

YES X NO

*The following are examples of personally identifiable information:

- Name of an individual
- Date and place of birth
- Address

- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

The Electronic Medical Record (EMR) System establishes the essential medical record infrastructure that the Department of State must have to provide quality health care services for all U.S. Foreign Affairs agencies worldwide. The EMR establishes a single authoritative source of information that is readily retrievable for: patient care; medical evacuations and hospitalizations; medical clearance decisions; medical record release actions; medical program planning and management; and immunization tracking. The EMR converts existing paper medical record data to electronic data. The EMR provides a standard, rapid and secure way to enter new medical record information into a patient's Department of State medical record. Medical records on a patient, which are fragmented on paper in many geographically disparate locations, will be available for use in one secure and integrated medical record electronically.

3) What legal authority authorizes the purchase or development of this system/application?

Legal authority to procure a design and development of an electronic record system is derived from the Government Paperwork Elimination Act (GPEA), the Paperwork Reduction Act (PRA), and the e-Government Act of 2002.

C. DATA IN THE SYSTEM:

1) Does a Privacy Act system of records description already exist?

YES X NO

If yes, please provide the following:

System Name: Medical Records Number: State-24

If no, a Privacy system of records description will need to be created for this data.

2) What categories of individuals are covered in the system?

Foreign Service, eligible family member (EFM) and Civil Service employees working at overseas posts.

3) What are the sources of the information in the system?

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

The information contained in EMR is taken from the individual. The medical information contained in the EMR system is derived via interview sessions with each patient and medical examinations of each patient.

- b. Why is the information not being obtained directly from the individual?**

Not applicable.

- c. What Federal agencies are providing data for use in the system?**

Not applicable.

- d. What State and/or local agencies are providing data for use in the system?**

Not applicable.

- e. From what other third party sources will data be collected?**

Individuals have the option of having a third party physician complete their physical. As such, the medical information obtained from the third party physician is contained in EMR.

- f. What information will be collected from a State Department employee and the public?**

Medical and demographic information is collected from State Department employees and eligible family member (EFM).

3) Accuracy, Timeliness, and Reliability

- a. How will data collected from sources other than DOS records be verified for accuracy?**

MED medical professionals use medical professional protocols. These protocols include quality review to ensure that the information in the system is accurate. Information that is collected from other sources is processed through the medical records scan and review process. This includes scanning hard copies of medical examinations and

documentation, performing quality checks of the scanned records for accuracy, and performing final quality review by each medical professional who views the information collected.

b. How will data be checked for completeness?

See the response above.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The data in the system is current as of the last interaction/communication with the individual.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail and documented both in the system and in the system requirements document.

D. DATA CHARACTERISTICS:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Yes, the system can derive new data or create previously unavailable data about an individual through aggregation via the reporting mechanism. These reports are maintained separately in the system database.

3) Will the new data be placed in the individual's record?

Yes.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No.

5) How will the new data be verified for relevance and accuracy?

Not applicable.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

EMR components used by Department of State medical personnel are dependent upon access control. Access control authorizes individual module specific access rights and valid user authentication. The EMR login process is a two-tiered process. The login validates a user's security identifier (user name) and access rights/roles permissions within the EMR system. Within each module of eMED, each user has a specific role and permissions that apply to the function of that role within the eMED database. When a user logs on, his or her user name and password are checked against the username within the Oracle database. If the username correlates to one on file, application specific access rights are granted to the user. Users are forced to change passwords every 180 days by system administrators. Users are not allowed to manually change passwords without the prompting of a system administrator.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

See answer above.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data may be retrieved from the EMR system using the patient's name, social security number, date of birth and patient ID.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

EMR has the capability to deliver multiple types of reports. The reports will be used to examine trends in medical care delivery, medical condition, health awareness and epidemiology. Only Department of State medical personnel will have access to these reports based on the access control guided by their business roles.

In case of emergency, the reports will be provided to the proper authority on a "need to know basis". following the HIPAA rule.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Not applicable

- 2) What are the retention periods of data in this system?**

The retention period for active employees and eligible family members is through the duration of the individual employment or eligibility of family member under the medical program. Retention of data for separated employees and eligible family members is retained indefinitely.

A records disposition schedule must be created immediately. Please e-mail records@state.gov for assistance.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

When required, data will be disposed of as an individual record, with the disposition instructions taking effect once the employee has transferred or separated. Queries are run on a regular basis to determine which employees and family members data needs to be removed from the system. Results of queries and/or reports are kept for as long as it is required to assist in removing data from the system. Once the data removal is complete, all queries and reports are destroyed. As of this time, procedures are being finalized before documenting as a Work Instruction for Medical Informatics and Medical Records.

- 4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

- 5) How does the use of this technology affect public/employee privacy?**

Not applicable.

- 6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

The system will be able to identify individuals and their medical information, locate them based on their most recent physical, which indicates the overseas post to which they are assigned, and monitors any change in their medical condition.

7) What kinds of information are collected as a function of the monitoring of individuals?

For monitoring purposes, the only information collected and reported are items related to any change in an individual's medical condition.

8) What controls will be used to prevent unauthorized monitoring?

Medical professional standards dictate that any unauthorized use and monitoring of medical information for reasons other than primary care is unacceptable. With that said, access to EMR and any monitoring is based on the business role of all users given access to the system.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

Any changes to the system will not require a revision to the Privacy Act system of records notice, since any modifications will be within the same scope as the current system.

The system is not being modified

**11) Are there forms associated with the system? YES X NO
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?**

Each form does contain a Privacy Act statement that includes the required information identified by the Privacy Act regulation.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)

Contract and direct hire medical personnel and system administrators.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the system and data are determined by each individual's business need and role. The access rules have been identified in the EMR User Requirements documentation.

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

User access is determined by user role. If an individual's role does not require access to the system, they are restricted from accessing the system.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

The system is configured with full access auditing at the database level. This auditing records all events including the data accessed (and/or modified – and in the event of modifications – the original data state before modification), by whom, and the date and time at which each event occurred.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Contractors are involved with the design and development of the system. Each contract has Privacy Act clauses inserted, so that the contractors are aware of their responsibilities regarding privacy. Annual training is provided to all users and non-users of the system (as part of their security training) regarding the handling of sensitive information and information processing systems.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

A Human Resources interface exists between EMR and HR. Data is transmitted from EMR into an HR access database. The type of data being transmitted includes, last name, first name, middle initial, social security number, date of birth, registration date, external physical examination date, medical clearance determination, and the medical clearance date.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Dr. Robert Burney, Office of Medical Services Privacy Officer.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No.

9) If so, how will the data be used by the other agency?

No.

10) Who is responsible for assuring proper use of the data?

Dr. Robert Burney, Office of Medical Services Privacy Officer and Jim Thornberry, Office of Medical Services, ISSO.

ADDITIONAL COMMENTS: (optional)